UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/846,522	04/30/2001	Tomoyuki Nakano	112857-221	5535

29175 7590 08/23/2006

BELL, BOYD & LLOYD, LLC
P. O. BOX 1135
CHICAGO, IL 60690-1135

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/846,522	NAKANO ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *06 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/6/2006 has been entered.

Response to Arguments

2. In response to communications filed on 6/6/2006, applicant has amended claims 1, 5, 13, 14, 21, 22, and 23. The following claims 1-23 are presented for examination.

2.1 Applicant's arguments, pages 11-16, filed on 6/6/2006, with respect to the rejection of claims 1-23 have been fully considered, but they are not persuasive as amended. Applicant argues that Audebert describes signing a transaction with a private key but not encrypting a data item associated with an authentication request from the server an sending the encrypted data item to the server to be decrypted with a public key and compared with a copy of the data item at the server. Applicant's disclosure recites generating a digital signature sheet with a private key in response to a request from server 3 and sending it to the server which in turn decrypts the digital signature using the private key, which is similar to the process disclosed by Audebert. Applicant's disclosure does not disclose comparing with a data item at the server. Upon further

consideration, Applicant has not overcome the rejection by amending the claims, and claims 1-23 remain rejected in view of Audebert.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3.1 Claims 1, 5, 13, 14, 21, 22, and 23 and the intervening claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's disclosure fails to recite "an additional authentication request sent from the information processing apparatus and wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item, and wherein, only when the user has been authenticated in response to the additional authentication request, the authentication apparatus performs processing as recited in claims 1, 21, and 23. The specification, on the other hand, does not describe an additional authentication request from the information processing apparatus (server 3) nor the additional authentication request is sent only if the decrypted result corresponds to the first data item.

Therefore, the specification does not describe the steps above as claimed. Claims 13, 14, and 22 recite similar limitations. As mentioned above, there is no description of an additional authentication request from the information processing apparatus (server 3). Claims 1, 5, 13, 14, 21, 22, and 23 also recite comparing the decrypted result with the first data item, which is not disclosed in the disclosure. The specification merely states when the decryption is successfully performed, it is determined the legitimate user has requested the electronic priced information (page 10, lines 10-12).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,694,436 to **Audebert**.

As per claim 1, **Audebert** substantially discloses a user authentication system, comprising: an integrated circuit card that meets the recitation of a data holding medium for holding a common key unique to a user, used in a common-key encryption method, for example (see column 21, lines 17-21); for authentication between the data holding medium held by the user and a terminal module that meets the recitation of authentication apparatus (see column 26, lines 38-42); said authentication apparatus for holding the common key used in the common key encryption method and a private key corresponding to the user used in a public-key encryption method, for example (see column 21, line 45 through column 22, line 20); for authentication between the data holding medium and a server or PC to perform a service to the user (see column 11, lines 10-29; column 12, lines 56-69 and column 24, lines 39-61); an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for performing authentication by the public-key encryption method, for example (see column 11, lines 10-29; column 12, lines 42-69 and column 24, lines 39-61); wherein said authentication apparatus is configured to receive a first data item, wherein the first data item is associated with a first authentication request from said information processing apparatus and wherein said authentication apparatus is configured to authenticate the data holding medium by using the common key in response to the first authentication request (see column 21, lines 28-38); wherein said authentication apparatus is further configured to encrypt only if the data holding medium is authenticated in response to the first authentication request, the first data item using the private key associated with the user and to send the encrypted first data item to the information processing apparatus (see column 21, line 50 through column 22, line 20); wherein said information processing apparatus is configured to decrypt the encrypted

first data item using a public key associated with the user and to compare the decrypted result with the first data item (see column 22, lines 7-20); **Audebert** discloses that the authentication of the data holding medium can be performed using PIN, challenge/response or asymmetrical algorithm (see column 26, lines 25-45); wherein the authentication apparatus performs authentication, authenticating the data holding medium by using the common key used in the common key encryption method for the user held by the data holding medium, in response to an additional authentication request sent from the information processing apparatus, wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item (see column 21, line 59 through column 22, line 20); and, only when the user has been authenticated, in response to the additional authentication request the authentication apparatus performs processing using the private key corresponding to the user for making the information processing apparatus authenticate the user for example (see column 21, line 45 through column 22, line 20). **Audebert** discloses the authentication apparatus has means for authenticating the source and integrity of data received from the sender and further discloses using public-key encryption for secure communication (see column 23, lines 55 through column 24, line 22 and column 24, lines 23-64) that meets the recitation of wherein information encrypted by the public-key encryption method is sent from the information processing apparatus, forwarded to the authentication apparatus, decrypted using the private key corresponding to the user, so as to obtain decrypted information (see also column 21, lines 10-27 and lines 40-45 and column 25, lines 37-45); and discloses common key encryption method between the holding medium and the authentication apparatus that meets the recitation of wherein the decrypted information is encrypted means using the common key and wherein the obtained common key encrypted

information is sent back to the data holding medium (see column 24, lines 40-45). **Audebert** discloses a secure downloading in another embodiment wherein authentication apparatus performing processing using the private key corresponding to the user, this process of loading is performed upon assuring the integrity of the source and the user that requires an additional authentication request (see column 23, line 25 through column 24, line 38). **Audebert** clearly discloses the scope of the claimed invention as claimed and further suggests encrypting all data exchange between the modules (see column 24, lines 55-61) and further states encryption and signature mechanisms may be performed by any cryptographic techniques as known in the art (see column 12, lines 26-35). Although the steps are not explicitly disclosed with the exact orders as claimed, it would only require routine skill in the art to write the steps of the claimed invention using the encryption and authentication methods exchanged between the authentication apparatus, the holding medium, and information processing apparatus and the suggestions disclosed by **Audebert**. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have information processing apparatus encrypting data and forwarding it for verification to the authentication apparatus since **Audebert** suggests that the holding medium does not have the cryptographic capabilities for signature, that the authentication apparatus contains (column 21, lines 10-26) and if data is verified sending it to the holding medium as suggested by **Audebert** (columns 23-24). One of ordinary skill in the art would have been motivated to do so as suggested by **Audebert** in order to perform a secure downloading of information into the medium that includes mutual authentication of all the modules involved (see column 23, lines 1-27).

As per claims 2 and 6, **Audebert** discloses a user who carries an integrated circuit card that meets the recitation of a data holding medium that is portable (see column 21, lines 17-21).

As per claims 3, 9, and 19, **Audebert** discloses the limitation of wherein the information processing apparatus is a mobile communication apparatus, for example (see column 27, lines 5-18).

As per claims 4, 8, and 18, **Audebert** discloses wherein the data holding medium and the information processing apparatus are integrated as one unit (see column 11, lines 30-33).

As per claim 7, **Audebert** discloses wherein the user authentication request is sent from an information processing apparatus (see column 12, lines 47-55 and column 13, lines 45-46).

As per claim 5, **Audebert** substantially discloses a user authentication method for a user who carries an integrated circuit card that meets the recitation of a data holding medium for holding a common key unique to a user, used in a common-key encryption method, for example (see column 21, lines 17-21); for authentication between the data holding medium held by the user and a terminal module that meets the recitation of authentication apparatus (see column 26, lines 38-42) and a private key used in a public-key encryption method to the authentication between the data holding medium and a server or PC to perform a service to the user (see column 11, lines 10-29; column 12, lines 56-69 and column 24, lines 39-61); a method comprising: authenticating a data holding medium of a user by the common key encryption method using the

common key held by the data holding apparatus in response to an authentication request from the server (see column 13, lines 43-60 and column 26, lines 25-45); receiving a first data item wherein the first data item is associated with the authentication request from the server (see column 26, lines 25-45); and performing only when the data holding apparatus of the user has been authenticated processing for authenticating the data holding apparatus of the user by a public-key encryption method (see column 26, lines 25-45 and column 21, line 45 through column 22, line 20); receiving a second data item, wherein the second data item is encrypted by the server using the public-key of the user: decrypting the second data item using the private-key of the user; encrypting the decrypted second data item using the common key: and sending the result of encrypting the decrypted second data item to the data holding apparatus (see column 21, line 45 through column 22, line 20); and see also another embodiment in columns 23-24). Although the steps are not explicitly disclosed with the exact orders as claimed, it would only require routine skill in the art to write the steps of the claimed invention using the encryption and authentication methods exchanged between the authentication apparatus, the holding medium, and information processing apparatus and the suggestions disclosed by **Audebert**. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have information processing apparatus encrypting data and forwarding it for verification to the authentication apparatus since **Audebert** suggests that the holding medium does not have the cryptographic capabilities for signature, that the authentication apparatus contains (column 21, lines 10-26) and if data is verified sending it to the holding medium as suggested by **Audebert** (columns 23-24). One of ordinary skill in the art would have been motivated to do so as suggested by **Audebert** in order to perform a secure downloading of information into the

medium that includes mutual authentication of all the modules involved (see column 23, lines 1-27).

As per claims 10-11 and 16, **Audebert** discloses wherein the data holding apparatus is an IC card (see column 21, lines 17-21).

As per claim 12, **Audebert** discloses wherein the information processing apparatus has a communication function, a browser function for accessing information on the Internet and a reader and writer function for reading and writing the IC card (see column 12, line 56 through column 13, line 11).

As per claim 13, **Audebert** substantially discloses a user authentication method for a user who carries an integrated circuit card that meets the recitation of a data holding medium for holding a common key unique to a user, used in a common-key encryption method, for example (see column 21, lines 17-21); for authentication between the data holding medium held by the user and a terminal module that meets the recitation of authentication apparatus (see column 26, lines 38-42) and a private key used in a public-key encryption method to the authentication between the data holding medium and a server or PC to perform a service to the user (see column 11, lines 10-29; column 12, lines 56-69 and column 24, lines 39-61); receiving a first data item wherein the first data item is associated with the authentication request from the server (see column 26, lines 25-45); and performing only when the data holding apparatus of the user has been authenticated in response to the first authentication request processing for authenticating

the data holding apparatus of the user by a public-key encryption methods wherein the processing includes encrypting the first data item using a private-key of the user and sending the encrypted first data item to the server, wherein the server decrypts the encrypted first data item using a public-key of the user and compares the decryption result with the first data item: processing for authenticating the data holding apparatus of the user by a public-key encryption method (see column 13, lines 43-60 and column 21, line 45 through column 22, line 20); **Audebert** discloses that the authentication of the data holding medium can be performed using asymmetrical algorithm (see column 26, lines 25-45); authenticating in response to an additional authentication request sent from the information processing apparatus, the data holding apparatus by using the common key used in the common key encryption method for the user (see column 21, line 59 through column 22, line 20); and, only when the user has been authenticated, in response to the additional authentication request the authentication apparatus performs processing using the private key corresponding to the user for making the information processing apparatus authenticate the user for example (see column 21, line 45 through column 22, line 20). **Audebert** discloses the authentication apparatus has means for authenticating the source and integrity of data received from the sender and further discloses using public-key encryption for secure communication (see column 23, lines 55 through column 24, line 22 and column 24, lines 23-64) that meets the recitation of wherein information encrypted by the public-key encryption method is sent from the information processing apparatus, forwarded to the authentication apparatus, decrypted using the private key corresponding to the user, so as to obtain decrypted information (see also column 21, lines 10-27 and lines 40-45 and column 25, lines 37-45); and discloses common key encryption method between the holding medium and the authentication

apparatus that meets the recitation of wherein the decrypted information is encrypted means using the common key and wherein the obtained common key encrypted information is sent back to the data holding medium (see column 24, lines 40-45). **Audebert** discloses a secure downloading in another embodiment wherein authentication apparatus performing processing using the private key corresponding to the user, this process of loading is performed upon assuring the integrity of the source and the user that requires an additional authentication request (see column 23, line 25 through column 24, line 38). **Audebert** clearly discloses the scope of the claimed invention as claimed and further suggests encrypting all data exchange between the modules (see column 24, lines 55-61) and further states encryption and signature mechanisms may be performed by any cryptographic techniques as known in the art (see column 12, lines 26-35). Although the steps are not explicitly disclosed with the exact orders as claimed, it would only require routine skill in the art to write the steps of the claimed invention using the encryption and authentication methods exchanged between the authentication apparatus, the holding medium, and information processing apparatus and the suggestions disclosed by **Audebert**. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have information processing apparatus encrypting data and forwarding it for verification to the authentication apparatus since **Audebert** suggests that the holding medium does not have the cryptographic capabilities for signature, that the authentication apparatus contains (column 21, lines 10-26) and if data is verified sending it to the holding medium as suggested by **Audebert** (columns 23-24). One of ordinary skill in the art would have been motivated to do so as suggested by **Audebert** in order to perform a secure

downloading of information into the medium that includes mutual authentication of all the modules involved (see column 23, lines 1-27).

Claim 14 recites the similar limitations as claim 13 except for using implementing the claimed method of claim 13 in an authentication apparatus. Therefore claim 13 is rejected on the same rationale as the rejection of claim 13 and claim 1 (for also disclosing an authentication apparatus).

As per claim 15, **Audebert** discloses wherein the authentication apparatus has a a private key used in a public-key encryption method, (see column 21, line 45 through column 22, line 20).

As per claim 17, **Audebert** discloses wherein the information processing apparatus has a reader and writer function for reading and writing the IC card (see column 12, line 56 through column 13, line 11).

As per claim 20, **Audebert** discloses wherein the information processing apparatus has a communication function, a browser function for accessing information on the Internet (see column 12, line 56 through column 13, line 11).

Claims 21, 22 and 23 disclose similar limitations as the rejected claim 1 and are therefore rejected on the same rationale as the rejection of claim 1.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
August 18, 2006

NASSER MOAZZAMI
PRIMARY EXAMINER

8/21/06